



The Security Benefits Delivered by an ATM as a Service Solution

July 2023

ATM Authors:

Shpend Ibraimi, Executive Director – ATM as a Service for North America, NCR Corporation
Max Garcia, CISO, Global Banking Division, NCR Corporation

For more information visit [ncr.com](https://www.ncr.com)



Security threats can emerge very quickly, requiring rapid responses to mitigate losses and customer impacts.



Executive Summary

The reframing of banking services as a seamless experience across all channels is driving significant changes in the ATM market¹. Self-service technologies are a key component of digital banking strategies. ATMs are increasingly deployed in lieu of full-size branch expansions as an effective means of entering new regional markets, offering customers convenient, local access to their accounts, and promoting new products and services with in-stream marketing capabilities.

In the shadow world of financial services criminals, these same dynamics are in play, which means that now, more than ever, ATM security is critical – and expensive. New security threats require financial institutions to regularly monitor and upgrade their physical ATM devices, data and processing systems, PC core and software, PIN pad encryption, physical security protections and more to stay a step ahead of the criminal element.

Institutions must contend with the significant risk of cash loss and potentially even more damaging reputational risk as customers increasingly rely on ATMs for basic banking services. Financial institutions require a multi-layered approach to deploying security measures and managing risk in their ATM channel, an approach that is challenging for most financial institutions to fully deploy.

Threat trends indicate that criminals are becoming more aggressive in their physical and digital (logical) attacks on ATMs. Security threats can emerge very quickly, requiring rapid responses to mitigate losses and customer impacts.

While ATM security is important in its own right, it doesn't operate in a vacuum. To be effective, risk management controls are embedded across all system and network processes. This calls for tight alignment of ATM configurations and ongoing maintenance managed by security experts. The complexity of operating both an on-site and a remote ATM channel can significantly increase costs if these services are not cohesively managed in an already homogenized operating environment.

The ATM as a Service model takes into consideration all aspects of ATM channel management, including security, while simultaneously shifting a CapEx expense to a steady OpEx cost. Even more importantly, financial institutions that consolidate services under one ATM as a Service provider free up resources to focus on what's most important: higher levels of customer engagement.

¹ For purposes of this analysis, the "ATM market" includes both ATM and ITM devices.

The Risk of Under-Investment in ATM Security

ATM-related fraud losses are rising around the globe. In Europe during the first six months of 2020, ATM malware and logical attacks increased at an astounding 269% or from 35 to 129. These attacks translated into European bank losses increasing from €1,000, to just over €1 million.ⁱⁱ The South African Banking Risk Information Center reported an 11% increase in ATM attacks during 2021, resulting in a 17% increase in losses.ⁱⁱⁱ In Australia, the Australian Payments Clearing Association reported that in 2021, skimming fraud at ATMs cost over \$2.3 million.^{iv}

This increase in ATM fraud around the world means financial institutions are also at increased risk of losing more customers. The ability to deliver secure banking services lies at the heart of consumers' trust in financial institutions. ATMs represent the institution's brand to its market and should a consumer feel unsafe transacting, or see an ATM that's been physically compromised, it's the institution's reputation that suffers. In a recent EY survey of global banking customers^v, 81.9% completely or mostly trust their primary financial provider. The same study also found that **privacy/trust benefits outweighed all other benefits** as the main factor influencing a consumer's decision in selecting a bank.

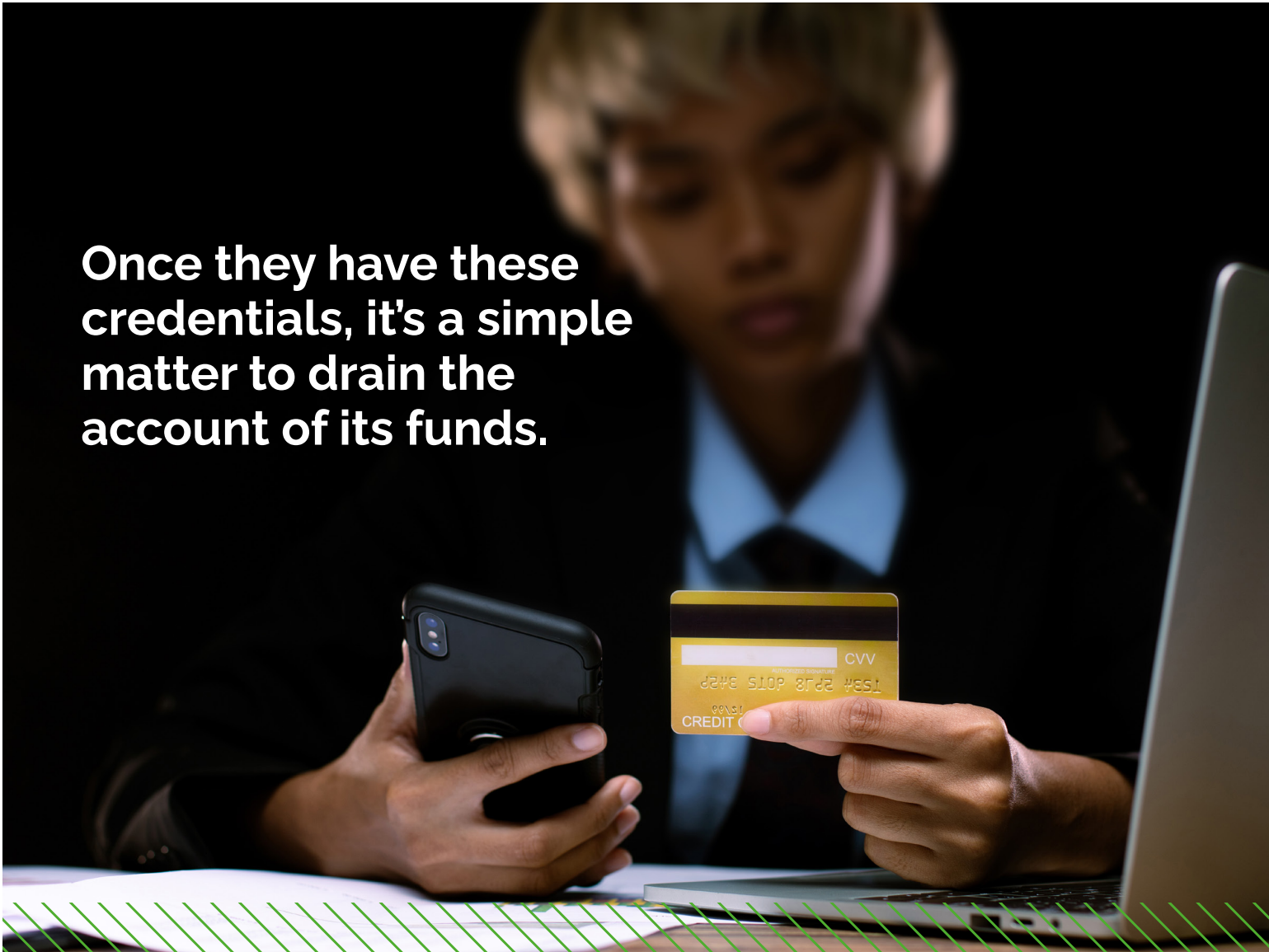
These global statistics illustrate that financial institutions whose ATM fleets and their operating environments are not properly

secured or whose organizations are not prepared to identify and react to emerging threat trends are at increased risk on multiple levels. There is the risk of monetary loss which is rising year over year. Then there is the physical risk to their operating environments highlighted by the extreme measures criminals will take to smash, drag, or blow-up ATMs. ATMs also run the risk of malware being "injected" into their software systems.

The most important threat is to consumer confidence, which can be quickly lost when the banking system is compromised. Acquiring and retaining customers in a hyper-competitive banking environment means each and every account matters.

\$81,000 average reported loss in the U.S.

The FBI's Bank Crime Statistics reports that ATM thefts – where the perpetrators were arrested – have risen from 31 in 2019 to 254 in 2021. The average reported loss is US\$81,000 or over US\$20 million nationwide.ⁱ

A person in a dark suit and light blue shirt is sitting at a desk. They are holding a black smartphone in their left hand and a gold credit card in their right hand. A laptop is open in front of them. The background is dark. The text 'Once they have these credentials, it's a simple matter to drain the account of its funds.' is overlaid on the left side of the image.

Once they have these credentials, it's a simple matter to drain the account of its funds.

Threat Trends

As ATM networks and software security protections become more advanced, fraudsters are turning their attention to physical device vulnerabilities. One result of this trend is that security threats and prevention measures have become similar around the world. For example, skimming attacks have evolved to leverage 3D printers that create false devices sometimes deployed along with pinhole cameras. This is how criminals are able to capture both card data and the PIN used to access the account. Once they have these credentials, it's a simple matter to drain the account of its funds.

Also on the rise are physical cash access attacks on ATM devices, where the criminal removes the ATM from its foundation to empty its contents elsewhere. These physical brute force attacks can be especially costly since they often result in the loss of the ATM, the loss of cash and significant damage to the surrounding structure or building. Successful ATM removal attacks breed more attempts as criminals learn the methods that work and locations/institutions with the weakest security controls.

There are a variety of criminal actors that may target ATMs, each with their own preferred attack routes and potential impacts. In Figure 1, we define the main criminal actors, what motivates them, and how a financial institution is impacted by their activities:

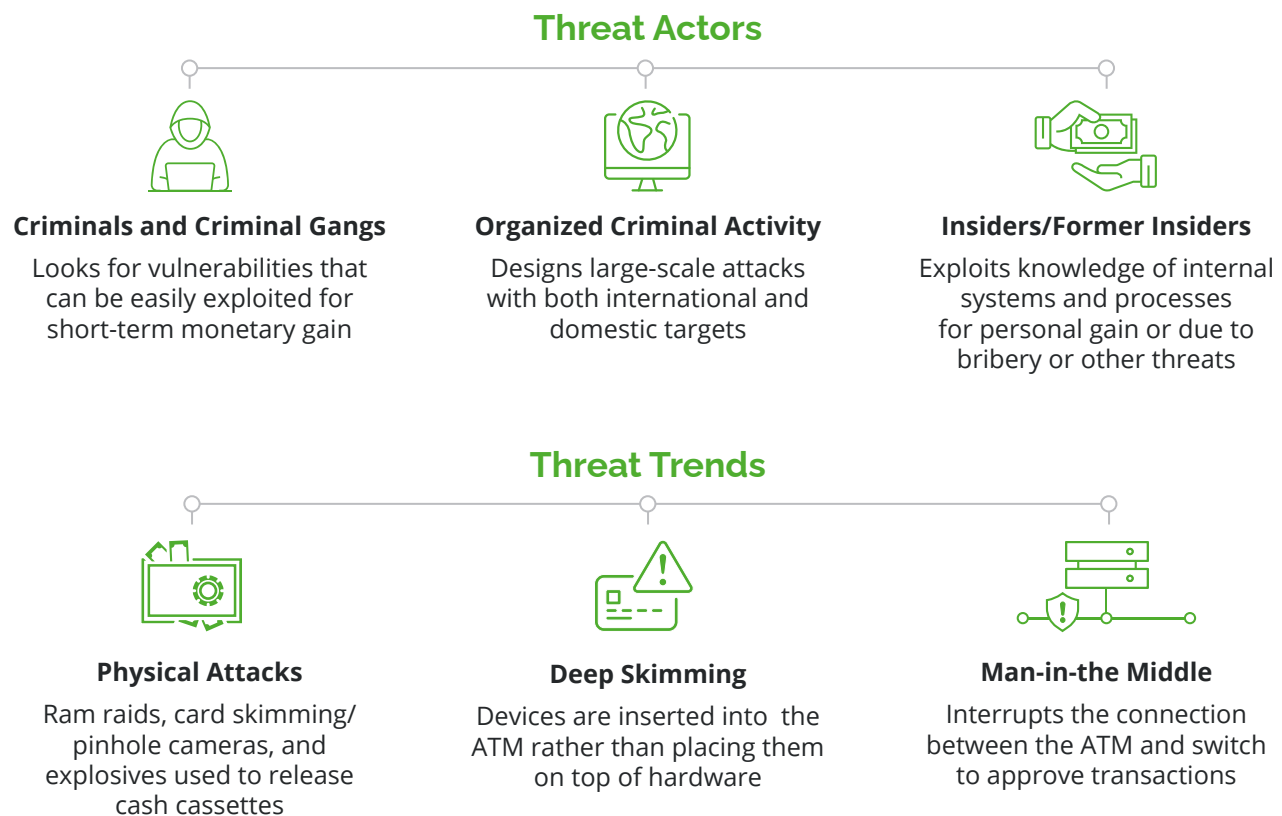


Figure 1: Threat Actors and Trends

Physical attacks present an institution with obvious remedies, like a bollard gate. However, digital attacks present a much more complex problem to institutions. One that requires deeper security expertise to resolve. Keeping up with digital-focused criminals means financial institutions must continually harden their internal and external software and keep a close eye on malware trends, network weaknesses, and new attack strategies. For example, criminals will phish

financial institution staff to try and obtain a password for a system used to manage/support ATM operations, then insert malware code or capture administrative access to jackpot the devices.

To mitigate these threats, financial institutions that manage their own ATM networks must continually invest in their technology. This investment includes, but is not limited to, using the latest encryption techniques and

Penetration Testing to protect ATM hard disks and dispenser communications, limiting access to USB ports, maintaining current anti-virus protections, and keeping operating systems fully locked down. These activities are costly and complicated. This challenge is compounded in countries where network connectivity is less developed, making it more difficult to install and maintain software security or even keep cameras recording.

Impact Costs

According to a recent ATM Crime Task Force Report published by the Texas Bankers Association^{vi}, banks participating on the Task Force... “report that just one or two of these crimes can lead to losses into the multiple six figures for an individual bank.” But there’s worse news, from a recent Morning Consult survey of consumer sentiment related to the most trusted brands in financial services.^{vii} Respondents to the survey indicated that the financial services industry was of particular concern, with roughly one third of respondents who lost trust in a financial services provider indicating they would never use that provider again, the highest percentage of all industries.

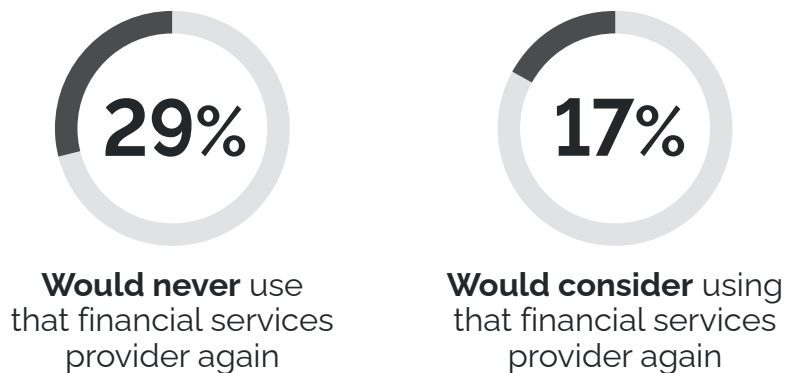
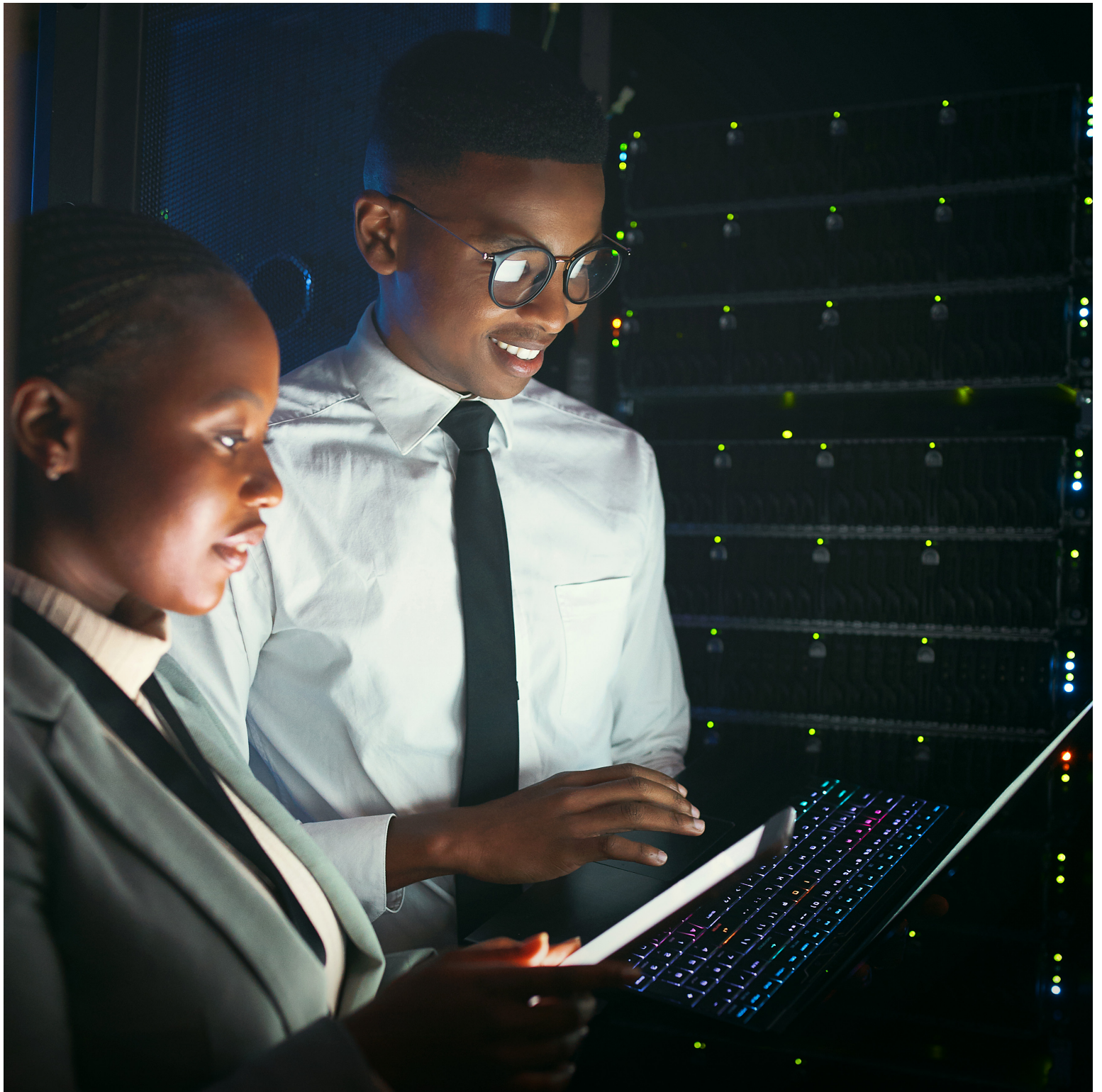


Figure 2: Morning Consult survey conducted April 8-14, 2022

Customers that are exposed to ATM criminal activity, whether directly or indirectly, may see that institution as less trustworthy. This is a significant issue for any institution as it presents the potential loss of that customer’s entire lifetime value.

What is an ATM Phishing Attack?

Through the use of social engineering (the tactic of manipulating, influencing, or deceiving a victim in order to gain control over a computer system), fraudsters can target financial institution employees to get them to open a malicious attachment. Once opened, the malware code is executed and infects the entire financial institution’s network and its endpoints, including ATMs. The ATM then becomes a slave machine that criminals can send instructions to for it to dispense money and then have money mules collect.



Maintaining a highly secure ATM environment requires constant capital and resource investments that place a high burden on retail banking operations.



The Building Blocks of Highly Effective ATM Security Solutions: Are You Ready?

A typical ATM operating eco-system is a complex mix of hardware, software, and business processes, all with potential points of vulnerability for criminals to exploit. Maintaining a highly secure ATM environment requires constant capital and resource investments that place a high burden on retail banking operations. Additionally, effective security means maintaining the capability to react in real-time as threats present themselves. Creating a secure ATM operating environment also means creating controls that can operate as building blocks to effectively catch and/or trap criminal activity before accounts can be compromised and reputational losses occur.

Attack Vectors

To create a secure operating environment for your ATM eco-system, a financial institution should be familiar with the attack vectors criminals use to gain access to devices. They fall into two main categories: physical and logical.



PHYSICAL ATTACK VECTORS target the device and its surrounding environment. For example, criminals may install hardware like skimming devices or try to break into devices using brute force.



LOGICAL ATTACK VECTORS target computer systems, applications, networks, and data. For example, criminals deploy technology such as malware to enable jackpotting or man-in-the-middle attacks.

What is an Attack Vector?

An attack vector is a path or means by which a criminal or hacker can gain access to a physical ATM, computer, or network server to deliver a payload or malicious outcome. Attack vectors enable hackers to exploit hardware and software system vulnerabilities, including the human element.

A Multi-Layer Security Approach

Best practices in ATM security management indicate that a multi-layered approach to protecting an ATM operating eco-system offers superior risk management controls (Figure 3). These controls should be centered around the ATM processing systems, software, and data as well as back-office operations. Taken together, these are the building blocks security experts have found to be most effective in maintaining an ATM operating environment that offers the highest levels of protection for financial institutions and their customers.

ATM SECURITY LAYERS

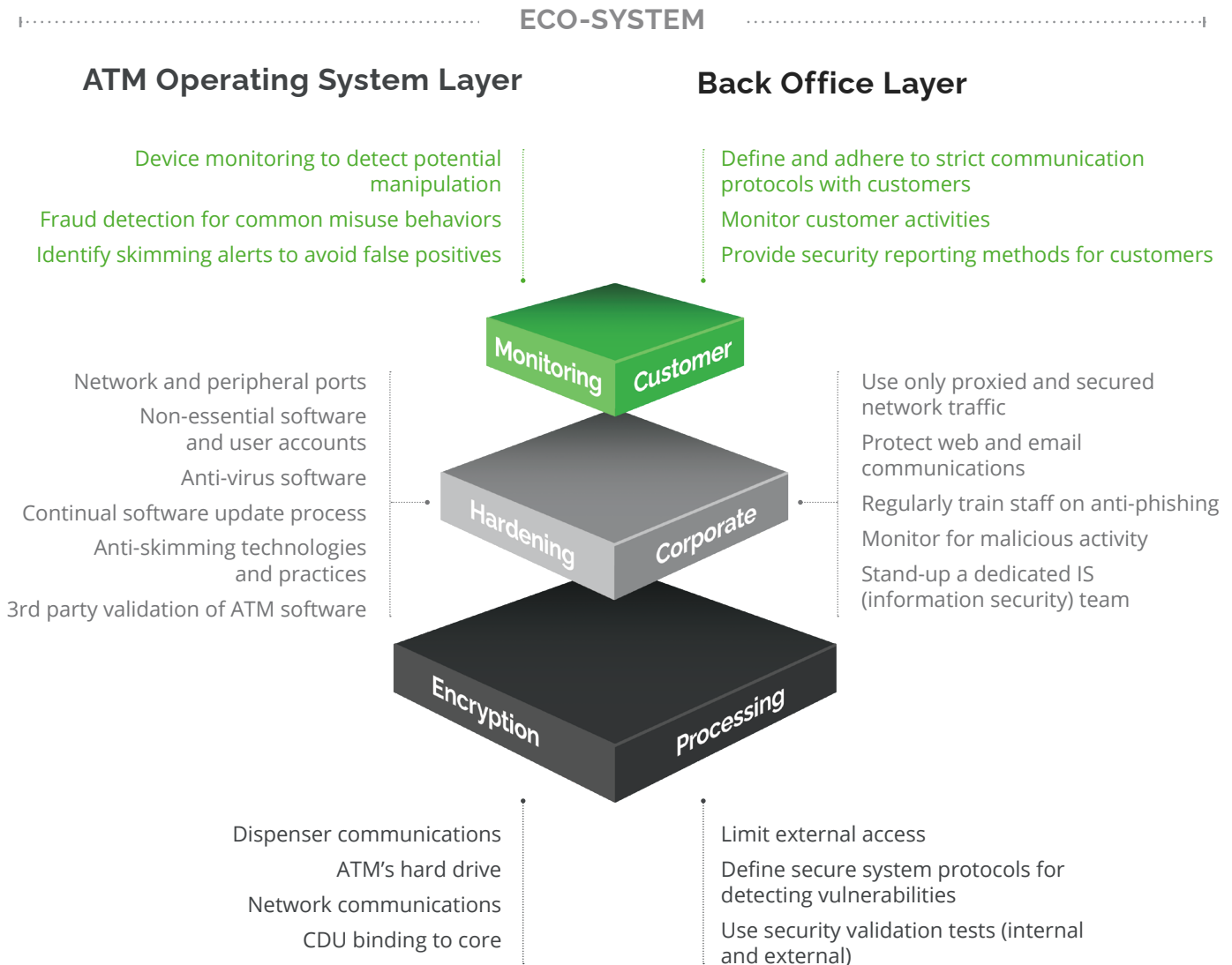


Figure 3: Multi-Layer ATM Security Approach

The multi-layer approach to ATM channel risk management, while highly effective, is also complicated and expensive to maintain. In addition, security must be integrated within the channel's entire environment. Financial institution leaders continually make decisions on how best to deploy capital against these needs. However, by compartmentalizing risk investments, an institution may miss vulnerabilities as each new ATM channel operating expense is scrutinized within the context of the financial institution's other investment needs. In addition, the complexity of risk management requires maintaining deep resource expertise, putting the institution in competition with many others wanting to hire the same types of resources.

Preventing Attacks Through Informed Investments

We know ATMs are physical 'honey pots' and require multiple physical and logical security layers to reduce risk and create effective deterrence controls. However, establishing and maintaining controls is no longer sufficient. Fraudsters' evolving tactics require additional capital and resource investment to protect the ATM channel. This means that financial institutions should be continually monitoring risk trends and modifying protections as required.

In addition, financial institutions wanting to enable new networks for their customers must be cognizant of these networks' initial weaknesses and ensure they are not exposing their systems or customers to increased risk until the network matures.

Is your institution frequently enabling new ATM features? Each new feature must be assessed from a risk perspective, requiring security, penetration and threat testing as key parts of the development lifecycle. Furthermore, as in the case of the new expanded BIN requirements for example, all systems and controls must be regression-tested to ensure existing protections aren't compromised by the new feature.

With a rapidly changing channel environment to contend with, financial institutions that wish to maintain a highly secure and responsive ATM eco-system must be prepared to expend capital and operating resources at increasing levels each year.

Fraudsters' evolving tactics require additional capital and resource investment to protect the ATM channel.

ATM Channel Outsourcing Addresses ATM Security Challenges

The challenging dynamics of ATM security, combined with the operational complexities of an ever more specialized channel, are motivating more financial institutions to re-assess their long-term ability to effectively operate the ATMs that are integral to their digital banking strategies. The question they ask is what is the best path forward to protect the financial institution from risk, while at the same time offering a robust, competitively differentiated self-service banking experience for customers?

Figure 4 identifies key questions for financial institutions to consider as they think about how best to create differentiated value within their ATM channel.



Adaptability, Sustainability and Affordability

How quickly can your institution incorporate new features and security measures?

What is your opportunity cost?



Analytics and Metrics

Do you have access to the data streams necessary to identify new or emerging fraud trends?



User Experience and Availability

Are your interfaces modern, accessible and easy to use?

Is your ATM hardware up-to-date, clean and fully functional?

Are your ATMs available 24x7?



Accessibility to Meet Market Demands

Is your institution able to deploy the ATMs it needs with the right service combinations where they're in the greatest demand?

Do you need to extend beyond your own branches to do so?

Figure 4: Value Differentiator Considerations

Additionally, financial institutions should factor into these decisions the potential financial impact of fraud losses and, even more importantly, loss of trust by customers. As stated earlier, just one ATM channel security incident could result in a six-figure direct loss of cash, hardware, and repair costs, while the reputational risk associated with security breaches, and the potential subsequent loss in clients, can be much more devastating.

A fully outsourced solution, or ATM as a Service (ATMaaS), is one way to solve this problem. ATMaaS shifts channel responsibility to the vendor, including upgrade and maintenance costs, security management and threat prevention across both physical and logical threats. Just like other As a Service options, ATMaaS delivers an ATM security eco-system that operates as an embedded best-in-breed solution within the ATM channel.

As you assess potential ATMaaS providers, here are a few questions to include in your due diligence process:

- Does your company maintain a team of highly experienced analysts and technologists whose job it is to analyze and react to risk trends in real-time across the globe?
- Are you making continuous investments into ATM Security R&D and at what level?
- Are you able to demonstrate increased operational efficiencies for your clients either through resource reallocation or improved loss prevention?

ATMaaS solutions are capable of managing both on- and off-premise devices, expanding the hardened security perimeter around an institution’s branded fleet (Figure 5) regardless of where these devices exist.

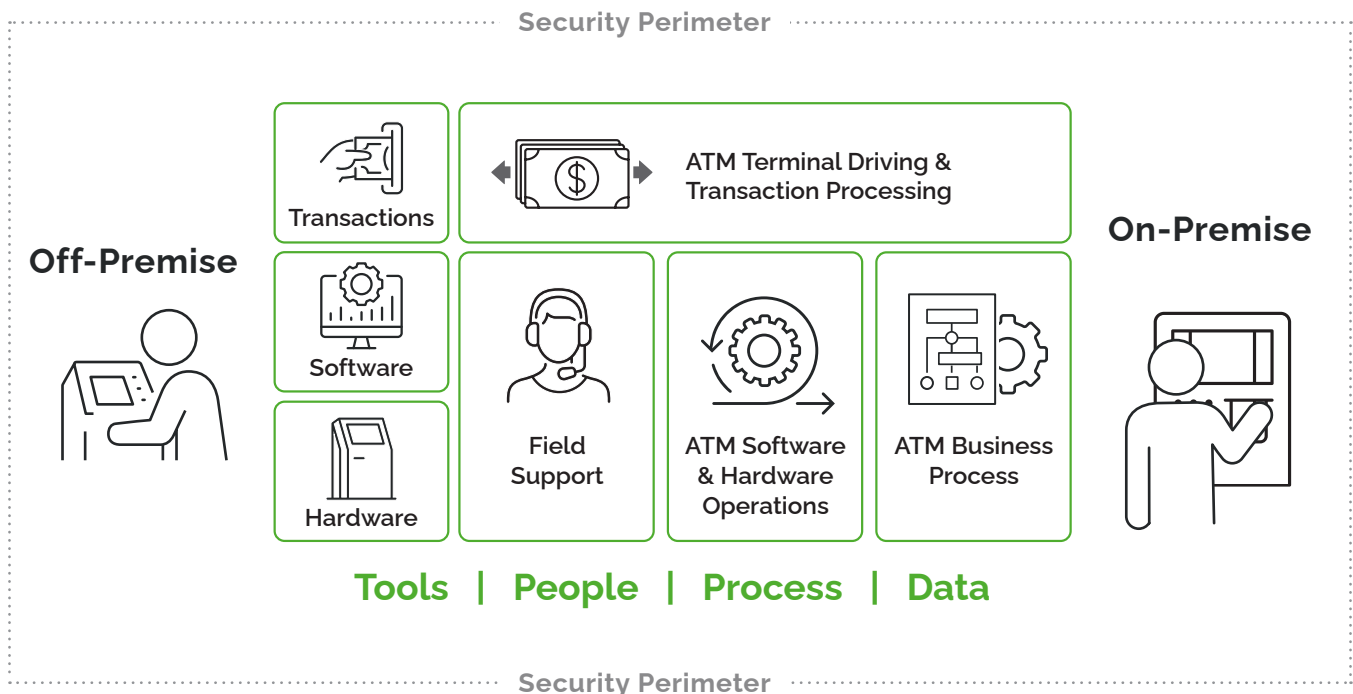


Figure 5: NCR ATM as a Service Solution



Protecting a Key Banking Channel

ATMs are the key link between digital banking services and the physical world. They can be a high-functioning component of differentiated services, but this channel brings its own unique set of risk management challenges. An ATM presents both a physical risk in its hardware and connectivity components and a logical risk in its software and networking components. For institutions that operate in developing regions of the world, these risks are amplified due to issues such as network immaturity, lack of rapid response capabilities and an evolving risk environment.

Security is but one piece of the ATM channel experience. The security eco-system lives within the larger ATM environment which points to the value a financial institution derives from working with an expert service provider that has embedded security across its processes. When an institution leverages ATM as a Service, it is able to both simplify management of this complex channel, freeing up resources for other priorities, and enhance the overall customer experience, including deployment of a highly secure channel.

All financial institutions are highly sensitive to protecting their consumers and brand. Losing brand trust is a serious and difficult

problem to solve. As criminals continue to devise better means of breaching ATM devices and their operating systems and networks, it is imperative that financial institutions continually invest financial and personnel resources in counteracting these threats. Yet, rationalizing this level of investment in a non-core business line is difficult at best.

ATM as a Service helps to better manage risk for financial institutions by leveraging expert services and their inherent benefits. With an expert service provider by their side, institutions can confidently turn their attention to areas of maximum strategic value.

A Proven Trust and Security Environment: The NCR Difference

As the owner/operator of the largest ATM fleet in the world, NCR has a unique perspective on the global ATM threat environment and security best practices to combat them. NCR invests millions of dollars of capital each year and dedicates significant resources to maintain the highest levels of channel security. NCR security teams are in regular contact with law enforcement officials at all levels around the world in order to proactively engage and thwart emerging threats. These are trust and security capabilities out of reach for most institutions, but available to our customers as part of our industry-leading ATM as a Service business.

Security is deeply integrated into our standardized software platform. This approach includes data, application, host, network and perimeter defense solutions that operate over and above OEM (original equipment manufacturer) software. NCR monitoring enables real-time reporting of device and/or application messages directly to operational and security management teams. Its distribution and inventory enable intelligent analysis of our terminal estate and rapid deployment of risk mitigation actions.

The NCR ATM security platform is built on best-in-breed technology including advanced cyber intelligence and forensic research. Our operating model addresses information security as a global independent function, and includes strategies to prevent large-scale data loss. The end result is that our financial institution customers are able to offer their customers industry-leading device availability in a highly secure environment.

ⁱ <https://www.claimsjournal.com/news/national/2022/08/09/312021.htm>

ⁱⁱ <https://www.association-secure-transactions.eu/black-box-attacks-increase-across-europe/>

ⁱⁱⁱ https://www.sabric.co.za/media/5dlnhnyj/sabric-crime-stats-2021_fa.pdf

^{iv} <https://pinkerton.com/our-insights/blog/atms-and-crime>

^v https://www.ey.com/en_gl/financial-services-emeia/how-traditional-banks-can-make-the-most-of-consumer-trust

^{vi} *ATM Crime Task Force Report, Texas Bankers Association, November 2020*

^{vii} <https://morningconsult.com/2022/06/21/federal-services-trust-data-privacy/>



NCR Corporation
864 Spring St. NW, Atlanta, GA 30308
Tel: +1-800-CALL-NCR | +1-937-445-1936
ncr.com